

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-306521
 (43)Date of publication of application : 02.11.2001

(51)Int.Cl. G06F 15/00
 G06F 12/00
 G06F 12/14

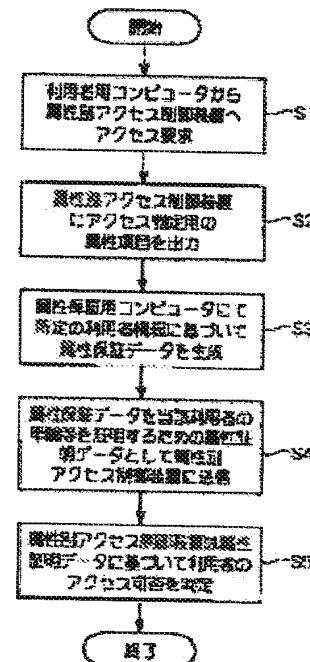
(21)Application number : 2000-119447 (71)Applicant : NEC CORP
 (22)Date of filing : 20.04.2000 (72)Inventor : IMOTO AKIO

(54) METHOD AND SYSTEM FOR CONTROLLING ACCESS BY ATTRIBUTES, AND STORAGE MEDIUM HAVING PROGRAM FOR AUTHENTICATION OR DATA FOR ACCESS CONTROL STORED THEREON

(57)Abstract:

PROBLEM TO BE SOLVED: To control access by the attributes of users, when receiving and transmitting information from and to a large number of unspecified users.

SOLUTION: When an attribute-dependent access controller is accessed from a user who uses a computer for users (S1), the attribute-dependent access controller transmits attribute items for deciding access propriety (S2). Subsequently, in a possible embodiment, the attribute items transmitted in the attribute item transmitting process S2 are received by the computer for users and then transmitted to the other computer. Furthermore, another computer generates attribute ensures data for guaranteeing the attribute of the relevant user on the basis of user information (S3). Subsequently, the computer for user transmits the attribute guarantee data generated in this attribute guarantee data generating process S3 to the attribute-dependent access controller as proof data for attribute for proving the attribute of the user (S4). On the basis of these attribute proof data, the attribute-dependent access controller decides the access propriety of the user, and when access is allowable, transmission/reception of information or the like is started (S5).



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-306521

(P2001-306521A)

(43)公開日 平成13年11月2日 (2001.11.2)

(51)Int.Cl.⁷

G 0 6 F 15/00
12/00
12/14

識別記号

3 3 0
5 3 7
3 1 0

F I

G 0 6 F 15/00
12/00
12/14

テマコード(参考)

3 3 0 D 5 B 0 1 7
5 3 7 A 5 B 0 8 2
3 1 0 K 5 B 0 8 5

審査請求 有 請求項の数10 O.L (全 15 頁)

(21)出願番号 特願2000-119447(P2000-119447)

(22)出願日 平成12年4月20日 (2000.4.20)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 井本 明夫

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100079164

弁理士 高橋 勇

F ターム(参考) 5B017 AA03 BA06 BB09 CA16

5B082 EA11

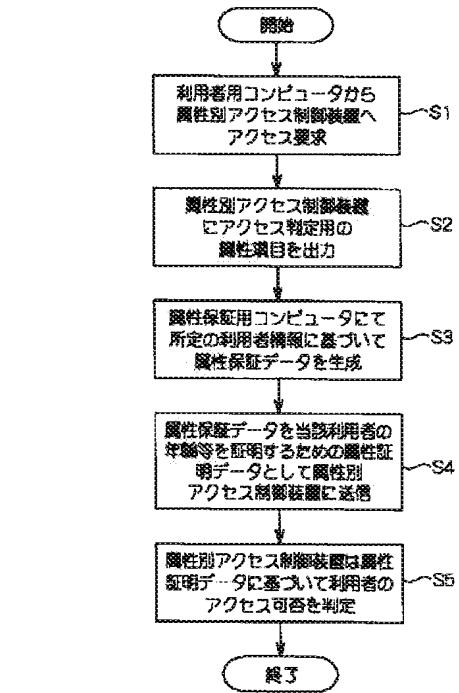
5B085 AA08 AE02 AE06

(54)【発明の名称】 属性別アクセス制御方法及びシステム並びに認証用プログラム又はアクセス制御用データを記憶した記憶媒体

(57)【要約】

【課題】 不特定多数の利用者に対して情報の受発信を行う際に利用者の属性別にそのアクセスを制御すること。

【解決手段】 利用者用コンピュータを使用する利用者から属性別アクセス制御装置にアクセスされたときに (S 1) 、当該属性別アクセス制御装置はアクセス可否を判定するための属性項目を送信する (S 2) 。続いて、ある実施形態では、属性項目送信工程 S 2 にて送信された属性項目を利用者用コンピュータで受信し、そして当該属性項目を他のコンピュータへ送信する。さらに、他のコンピュータは、当該利用者の属性を利用者情報に基づいて保証する属性保証データを生成する (S 3) 。続いて、利用者用コンピュータは、この属性保証データ生成工程 S 3 にて生成された属性保証データを利用者の属性を証明する属性証明データとして属性別アクセス制御装置に送信する (S 4) 。属性別アクセス制御装置は、この属性証明データに基づいて利用者のアクセスの可否を判定し、アクセスが可能であれば情報の送受信等を開始させる (S 5) 。



のデータ送受信部を介して前記利用者端末と送受信するデータ又はプログラムデータからなる提供データの全部又は一部と当該提供データに対して利用者の年齢や在住地域等の属性別にアクセス可否を定めた属性別アクセス制御データとを記憶した属性別提供データ記憶部と、前記利用者端末から前記データ送受信部に前記提供データへのアクセスが要求された場合に前記属性別アクセス制御データに基づいて当該要求された提供データのアクセスに必要な属性の項目を当該利用者端末へ通知する属性項目通知制御部とを備えたことを特徴とする請求項3記載の属性別アクセス制御システム。

10 【請求項5】 前記属性項目通知制御部は、前記利用者のアクセスを制御するセッションや一定期間等の単位毎に他の利用者と識別するアクセス管理用IDを前記利用者端末へ向けて送信させるアクセス管理用ID送信機能を備え、前記認証サーバーの要求属性データ認証部が、前記認証要求属性データに前記情報受発信サイトによって発行されたアクセス管理用IDを含めるアクセス管理用ID付加機能を備え、

20 【請求項6】 前記属性項目別アクセス制御部が、前記認証要求属性データのアクセス管理用IDを使用する利用者に対して前記アクセスの単位分のアクセス権限を与えるアクセスID別管理機能を備えたことを特徴とする請求項4記載の属性別アクセス制御システム。

【請求項7】 利用者が利用できる有線又は無線の通信回線をインターネット網に接続するインターネット接続手段と、前記利用者の氏名や年齢等の利用者個人情報を利用者識別用の利用者IDを単位として蓄積した利用者情報蓄積手段と、前記利用者の個人情報の一部を前記利用者の属性として認証する認証手段とを備え、

30 前記認証手段が、前記利用者が利用する利用者用端末から当該利用者の所定の属性についての証明要求を受信した時に前記利用者情報から当該要求された属性に関する要求属性データを抽出する要求属性データ抽出部と、この要求属性データ抽出部によって抽出された要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証する要求属性データ認証部と、この要求属性データ認証部によって認証された認証要求属性データを外部出力する認証要求属性データ出力部とを備え、前記認証手段が、前記利用者が利用する利用者用端末から当該利用者の所定の属性についての証明要求を受信した時に前記利用者情報から当該要求された属性に関する要求属性データを抽出する要求属性データ抽出部と、この要求属性データ抽出部によって抽出された要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証する要求属性データ認証部と、この要求属性データ認証部によって認証された認証要求属性データを外部出力する認証要求属性データ出力部とを備えたことを特徴とするプロバイダシステム。

40 【請求項8】 ネットワークに接続されると共に利用者の属性別の個人情報を格納した利用者情報を管理する利用者情報管理部を備えたサーバー用コンピュータを使用して前記ネットワークを介して接続される利用者用コンピュータの前記利用者の属性を認証するための属性認証用プログラムを記憶した記憶媒体であって、該属性認証用プログラムは前記サーバー用コンピュータを動作させる指令として、

前記利用者用コンピュータから送信された当該利用者の全属性のうちの一部の属性について証明を要求された場

【特許請求の範囲】

【請求項1】 複数の利用者用コンピュータとネットワークを介して接続され前記利用者に関連する属性別に当該利用者からのアクセスを制御する属性別アクセス制御装置と、前記ネットワークを介して前記利用者用コンピュータと接続され前記属性別アクセス制御装置からは読み出せない状態で保管された予め定められた利用者情報を管理する他のコンピュータとを使用して利用者のアクセスを制御する属性別アクセス制御方法であって、前記利用者用コンピュータを使用する利用者から前記属性別アクセス制御装置にアクセスされたときに当該属性別アクセス制御装置はアクセス可否を判定するための属性項目を送信する属性項目送信工程と、この属性項目送信工程にて送信された属性項目について前記他のコンピュータは当該利用者の属性を前記利用者情報に基づいて保証する属性保証データを生成する属性保証データ生成工程と、この属性保証データ生成工程にて生成された属性保証データを前記利用者用コンピュータは前記利用者の属性を証明する属性証明データとして前記属性別アクセス制御装置に送信する属性証明データ送信工程とを備えたことを特徴とする属性別アクセス制御方法。

【請求項2】 前記属性保証データ生成工程は、前記属性項目に前記利用者を識別する属性が含まれない場合には前記利用者情報中の当該利用者を識別する利用者ID等の属性項目データを前記属性保証データに含めない状態で当該属性保証データを生成する匿名保持属性保証工程を備えたことを特徴とする請求項1記載の属性別アクセス制御方法。

【請求項3】 利用者用端末とネットワークを介して接続され前記利用者端末からアクセスされる情報受発信サイトと、前記利用者端末と前記ネットワークを介して接続され前記利用者用端末を使用する利用者の属性が格納された利用者情報を管理する認証サーバーとを備えた属性別アクセス制御システムであって、

前記認証サーバーが、前記利用者用端末から当該利用者の所定の属性についての証明要求を受信した場合に前記利用者情報から当該要求された属性に関する要求属性データを抽出する要求属性データ抽出部と、この要求属性データ抽出部によって抽出された要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証する要求属性データ認証部と、この要求属性データ認証部によって認証された認証要求属性データを外部出力する認証要求属性データ出力部とを備え、前記情報受発信サイトが、前記認証要求属性データ出力部によって出力された認証要求属性データに基づいて当該利用者のアクセスの可否を判定する属性項目別アクセス制御部を備えたことを特徴とする属性別アクセス制御システム。

【請求項4】 前記情報受発信サイトが、前記利用者端末とのデータの送受信を制御するデータ送受信部と、こ

3
合に前記利用者情報管理部によって管理される利用者情報から当該要求された属性に関する要求属性データを抽出させる要求属性データ抽出指令と、
この要求属性データ抽出指令に応じて抽出される要求属性データ又は当該要求属性データに基づいた判定結果を認証させる要求属性データ認証指令と、
この要求属性データ認証指令に応じて認証される認証要求属性データを外部出力させる認証要求属性データ出力指令とを備えたことを特徴とする属性認証用プログラムを記憶した記憶媒体。。

【請求項8】 前記要求属性データ認証指令は、前記利用者用コンピュータから属性の証明をされる際にアクセス管理用IDが付されていた場合には当該アクセス管理用IDを前記認証要求属性データに当該アクセス管理用IDを含有させる指令を備えたことを特徴とする請求項7記載の属性認証用プログラムを記憶した記憶媒体。

【請求項9】 利用者用端末とネットワークを介して接続され前記利用者端末からアクセスされる情報受発信サイトと、前記利用者端末と前記ネットワークを介して接続され前記利用者用端末を使用する利用者の属性が格納された利用者情報を管理する認証サーバーとを備えた属性別アクセス制御システムにて使用され、前記利用者の匿名性を前記情報受発信サイトに保持しつつ前記利用者の属性に基づいて前記情報受発信サイトが利用者のアクセスを制限するための属性別アクセス制御用データを記憶した記憶媒体であって、

前記情報受発信サイトに前記利用者用端末を用いてアクセスした利用者に割り当てられるアクセス管理用IDデータと、前記情報受発信サイトによって特定された前記利用者用端末を使用する利用者の属性項目データと、この属性項目データにて指定される項目について前記認証サーバーの利用者情報から抽出された属性データと、前記各データの内少なくとも前記属性データの内容を前記認証サーバーにて認証したことを証明するための認証用データとを備えると共に、

前記認証サーバーによって認証された属性データは、前記情報受発信サイトにて前記アクセス管理用IDを用いた前記利用者のアクセス制限の判定に用いられることを特徴とした属性別アクセス制御用データを記憶した記憶媒体。

【請求項10】 利用者用端末とネットワークを介して接続され前記利用者端末からアクセスされる情報受発信サイトと、前記利用者端末と前記ネットワークを介して接続され前記利用者用端末を使用する利用者の属性が格納された利用者情報を管理する認証サーバーとを備えた属性別アクセス制御システムにて使用され、前記利用者の匿名性を前記情報受発信サイトに保持しつつ前記利用者の属性に基づいて前記情報受発信サイトが利用者のアクセスを制限するための属性別アクセス制御用データを記憶した記憶媒体であって、

4
前記情報受発信サイトに前記利用者用端末を用いてアクセスした利用者に割り当てられるアクセス管理用IDデータと、前記情報受発信サイトによって特定された前記利用者用端末を使用する利用者の属性項目データと、この各属性項目データに対して前記情報受発信サイトによってそれぞれ与えられる条件データと、この各属性項目データに対して与えられた条件データによる条件を満たしているか否かを前記認証サーバーの利用者情報に基づいて判定した属性項目別判定結果データと、前記各データの内少なくとも前記属性項目別判定結果データの内容を前記認証サーバーにて認証したことを証明するための認証用データとを備えると共に、
前記認証サーバーによって認証された属性項目別判定結果データは、前記情報受発信サイトにて前記アクセス管理用IDを用いた前記利用者のアクセス制限の判定に用いられることを特徴とした属性別アクセス制御用データを記憶した記憶媒体。

【発明の詳細な説明】

【0001】

20 【発明の属する技術分野】 本発明は、属性別アクセス制御方法及びシステムに係り、特に、利用者に関する情報の事前登録なく利用者の属性別にアクセスを制御する属性別アクセス制御方法及びシステムに関する。

【0002】

【従来の技術】 近年、TCP/IPによるインターネット（ネットワーク間通信網）が整備され、政府、企業、大学、個人などの有するコンピュータが直接又は電話回線網等を介して相互に接続されるようになった。インターネットを介して提供されている情報としては、各企業が製造する製品のデータ・シートや、新製品に関する情報や、行政により作成される文書や、作成中の法案や、最高裁判例の要旨や、大学の研究室の研究成果や、ある地域の宿泊施設の詳細情報や、ニュース、天気予報など、極めて多岐に渡る情報源からのものである。このような情報の受発信から、企業間取引（B to B）や、企業対顧客取引（B to C）等の商取引をインターネットを用いて行うための技術基盤が種々提案されている。

40 【0003】 インターネットを介して提供又は収集される情報は、マークアップ・ランゲージを用いて記述されたページ（例えば、HTMLページやXMLデータ）として作成されている。このページ（一般的には、ホームページと呼ばれる）をコンピュータや他の組み込みデバイスを使用して閲覧できるようになっている。インターネットを介した情報の受発信をクライアント・サーバーシステムとして構築すると、利用者クライアント（利用者が使用するコンピュータ）と、利用者クライアントとの通信を制御するWebサーバー（サーバー用プログラムを実装したコンピュータ）とを備えれば良い。各コンピュータは所定のプロトコル（例えば、httpやftp）で通信することで、ページやファイルの転送を行つ

ている。そして、商品データや画像データなどをデータベースに格納しておき、アクセスされたときのキーワード等からH T M Lページを自動生成し、利用者に表示したり、または、利用者に入力を促して、入力されたデータをデータベースに登録することも行われている。この場合、W e bサーバーは、利用者クライアントを他の利用者と識別しつつ通信を行い（セッション管理）、W e bサーバーに併設されたデータベースに格納されたデータを例えばS Q L文等により検索し、検索結果と予め定められた表示形式に基づいてH T M Lページを自動生成する。このような、インターネットを介して利用者用コンピュータ（利用者クライアント）や組込機器に情報を提供するW e bサーバーや、データベースが付随したW e bサーバーを、サイトと呼ぶことがある。

【0004】現状のインターネットを用いたサイトからの情報提供では、利用者からサイトにアクセスがあった場合であっても、サイト側で利用者の個人情報をることはできない。もちろん、通信上どのようなコンピュータからのアクセスなのかを知ることはできる。しかし、現に接続しているコンピュータの使用者（利用者）の性別や年齢や嗜好や現住所などの利用者の属性は、システム的に得ることができない。このため、サイトにてアンケートを行い、その内容を収集しても、あくまで匿名でサイトに訪れた人々の自己申告を信用するという前提でのデータとなる。また、例えば不特定多数の利用者に広く蒸留酒の種類を紹介するサイトにて、20歳以上の利用者にのみアクセスを許可したい場合には、「20歳以上ですか？」との質問を行い、イエスと答えた場合に実際の紹介ページに導くことができるだけで、20歳未満の利用者が20歳以上であると不正確な申告をした場合に、その申告が虚偽であることを見分ける手段はなかった。

【0005】

【発明が解決しようとする課題】しかしながら、上記従来例では、不特定多数に情報を受発信するサイトにて、利用者の自己申告が不正確である場合には、利用者の属性に応じたアクセス制御を行うことができない、という不都合があった。例えば特開平10-72846号公報には、W e bサーバに条件ファイルを置き、利用者コンピュータからクライアント証明書なるものを送付させ、条件判定を行う手法が開示されている。この公報記載の手法では、W e bサーバがブラウザにクライアント証明書記入画面を表示させた後、利用者に条件を記入させ、記入結果をクライアント証明書として扱っているため、証明された情報の確からしさは、利用者の自己申告に依存してしまう。すなわち、この従来例では、利用者が誤って実際と違う条件を記入してしまった場合や、あるいは、利用者が虚偽の条件を記入した場合には、不正確な情報を証明することとなってしまう、という不都合があった。

【0006】また、予め登録されたユーザーにのみパスワードを付与してアクセスを制限することで、個人にパスワードを付し、現にアクセスしている利用者の氏名等の個人情報を含む利用者の属性を正確に把握することはできる。例えば、特開平11-98488号公報には、双方向テレビにて、在住エリアや性別や年代等の個人情報をデータベースに登録しておき、視聴者の属性に関して一定の条件を満たす受信機に対してチラシ広告等の番組を供給する技術が開示されている。

10 【0007】しかしながら、この公報記載の手法では、双方向テレビの様に予め視聴者として契約を交わしておき、個人情報を登録できる場合のみ可能であり、不特定多数の利用者についてその属性に基づいて広告提供等の種々の処理を行うことはできない、という不都合があつた。

【0008】

【発明の目的】本発明は、係る従来例の有する不都合を改善し、特に、不特定多数の利用者に対して情報の受発信を行う際に利用者の属性別にそのアクセスを制御することのできる属性別アクセス制御方法及びシステムを提供することを、その目的とする。

【0009】

【課題を解決するための手段】そこで、本発明では、複数の利用者用コンピュータとネットワークを介して接続され利用者に関する属性別に当該利用者からのアクセスを制御する属性別アクセス制御装置と、ネットワークを介して利用者用コンピュータと接続され属性別アクセス制御装置からは読み出せない状態で保管された予め定められた利用者情報を管理する他のコンピュータとを使用して、利用者のアクセスを制御する。この本発明による属性別アクセス制御方法は、利用者用コンピュータを使用する利用者から属性別アクセス制御装置にアクセスされたときに当該属性別アクセス制御装置はアクセス可否を判定するための属性項目を送信する属性項目送信工程と、この属性項目送信工程にて送信された属性項目について他のコンピュータは当該利用者の属性を利用者情報を基づいて保証する属性保証データを生成する属性保証データ生成工程と、この属性保証データ生成工程にて生成された属性保証データを利用者用コンピュータは利用者の属性を証明する属性証明データとして属性別アクセス制御装置に送信する属性証明データ送信工程とを備えた、という構成を探っている。これにより前述した目的を達成しようとするものである。

40 【0010】利用者用コンピュータは、専用線や電話回線やC A T Vのケーブル等を介してインターネットなどの広域ネットワークに接続可能な機器であり、携帯用や家電製品に付随する組込機器を含む。ネットワークとしては、例えばインターネットが該当するが、特定の企業内のみで稼働するイントラネットや、また、T C P / I P以外のプロトコルで通信する特定のネットワークであ

7
っても良い。属性別アクセス制御装置は、利用者用コンピュータからネットワークを介して接続されるサーバー等のコンピュータ機器であり、好ましい実施形態では、情報の受発信をするサイトの一部を構成する。他のコンピュータは、好ましい実施形態では、利用者の属性の内容を保証するための認証サーバーであるが、属性別アクセス制御装置や利用者用コンピュータと論理的に切り離されているのであれば、属性別アクセス制御装置や利用者用コンピュータを実現するためのコンピュータを用いることもできる。

【0011】利用者の属性は、主に利用者自身の年齢や住所など利用者の属性を意味するが、利用者が使用する利用者用コンピュータ及びその周辺機器の属性や、企業等の組織名や部署名にてアクセスする場合には、これら組織の業種や規模などを利用者の属性として扱うようにしても良い。このように、利用者の属性は、情報の受発信を行うサイトにとって利用者の特徴を識別するために役立つ種々の内容を含む。この利用者の属性の名称を、属性項目という。属性項目の内容又は条件に対する論理型の記述を、好ましい実施例では属性値と呼ぶ。

【0012】属性項目送信工程では、利用者用コンピュータを使用する利用者から属性別アクセス制御装置にアクセスされたときに、属性別アクセス制御装置が、アクセス可否を判定するための属性項目を送信する。属性項目は、常に同一の項目でも良いし、アクセスを要求されたデータの種別に応じて変化させるようにしても良い。例えば、蒸留酒についてアクセスされた場合には年齢を属性項目とし、女性向けの被服についてアクセスされた場合には性別を属性項目としても良い。属性項目は、属性別アクセス制御装置によってアクセス制御されるサイトの情報内容と、サイトのポリシーとによって定まる。女性向け被服の場合に、例えば、男性の閲覧を不可とするのであれば、属性別アクセス制御装置は、属性項目として性別を送信し、その性別がどちらであるかによってアクセスを制御する。

【0013】属性保証データ生成工程では、属性項目が送信されると、他のコンピュータは、属性項目送信工程にて送信された属性項目について当該利用者の属性を利用者情報に基づいて保証する属性保証データを生成する。属性項目は、一旦利用者用コンピュータに送信するようにも良いし、属性別アクセス制御装置との通信中に利用者が他のコンピュータを特定するような場合には、属性別アクセス制御装置から他のコンピュータへ直接属性項目を送信するようにもよい。他のコンピュータは、利用者用コンピュータ又は属性別アクセス制御装置から直接又は間接的に送信された属性項目について、アクセスする利用者ID等を用いて利用者情報から属性の内容を保証する属性保証データを生成する。属性項目が単純な項目名として送信された場合には、その内容を属性保証データに含めれば良いし、一方、属性項目

についての条件を満たすか否かについて、例えばデータベースに対する問い合わせ文（SQL等）として送信された場合には、属性項目とその真偽を示す論理型を属性保証データに含めると良い。さらに、属性証明データ送信工程は、属性保証データ生成工程にて生成された属性保証データを利用者の属性を証明する属性証明データとして属性別アクセス制御装置に送信する。すなわち、利用者は属性別アクセス制御装置に対して利用者の属性の内容を証明するために、他のコンピュータにて保証された属性保証データを用いる。属性別アクセス制御装置は、他のコンピュータにて保証された属性内容に基づいて利用者のアクセスを制御する。また、好ましい実施形態では、属性保証データに利用者を識別するデータを含めない。すると、利用者は、匿名としながらその属性のみを属性別アクセス制御装置に送信することができる。

【0014】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。本実施形態では、複数の利用者用コンピュータとネットワークを介して接続され利用者に

20 関連する属性別に当該利用者からのアクセスを制御する属性別アクセス制御装置と、ネットワークを介して利用者用コンピュータと接続され属性別アクセス制御装置からは読み出せない状態で保管された予め定められた利用者情報を管理する他のコンピュータ（例えば、認証サーバーやプロバイダ用システム）とを使用して利用者のアクセスを制御する。属性別アクセス制御装置は、利用者用コンピュータを対象として情報の受発信を行う情報受発信サイトにて用いると、利用者の嗜好やコンピュータ使用歴などの利用者の属性別に情報の受発信を行うことができる。また、企業内のインターネット等のサーバーにて属性別アクセス制御装置を用いると、例えば無記名投票であるとか、匿名での応募やアンケートなどに応用することができる。

【0015】図1は本発明の一実施形態による属性別アクセス制御方法の構成を示すフローチャートである。本実施形態による属性別アクセス制御方法は、利用者用コンピュータを使用する利用者から属性別アクセス制御装置にアクセスされたときに（ステップS1）、当該属性別アクセス制御装置はアクセス可否を判定するための属性項目を送信する（ステップS2、属性項目送信工程）。続いて、ある実施形態では、属性項目送信工程S2にて送信された属性項目を利用者用コンピュータで受信し、そして当該属性項目を他のコンピュータへ送信する。さらに、他のコンピュータは、当該利用者の属性を利用者情報に基づいて保証する属性保証データを生成する（ステップS3、属性保証データ生成工程）。続いて、利用者用コンピュータは、この属性保証データ生成工程S3にて生成された属性保証データを利用者の属性を証明する属性証明データとして属性別アクセス制御装置に送信する（ステップS4、属性証明データ送信工

程）。属性別アクセス制御装置は、この属性証明データに基づいて利用者のアクセスの可否を判定し、アクセスが可能であれば情報の送受信等を開始させる（ステップS5）。

【0016】このように、利用者の属性の証明を本人の自己申告や実際にアクセスされたサーバーと切り離し、他のコンピュータにてその属性の内容を保証することとしたため、不特定多数の利用者に対して属性別のアクセス制御を行うことが可能となる。

【0017】また、好ましい例では、属性保証データ生成工程S3が、属性項目に利用者を識別する属性が含まれない場合には利用者情報中の当該利用者を識別する利用者ID等の属性項目データを属性保証データに含めない状態で当該属性保証データを生成する匿名保持属性保証工程を備えるようにしても良い。この場合、利用者は属性別アクセス制御装置に対して匿名を保ちつつ保証された属性データを送信することができる。

【0018】図2は、図1に示した属性別アクセス制御方法の使用に好適な属性別アクセス制御システムの実施の形態を示すブロック図である。図2に示す例では、利用者用端末とネットワークを介して接続され利用者端末からアクセスされる情報受発信サイト12と、利用者端末とネットワークを介して接続され利用者用端末を使用する利用者の属性が格納された利用者情報（個人情報ファイル）を管理する認証サーバー18とを備えている。利用者情報20は、物理的に認証サーバー18からアクセスされる状態で保管しても良いし、または、論理的にアクセス可能な状態としても良い。

【0019】利用者用コンピュータ10A、10B、10Cは、インターネット等のネットワークに多数接続されている。情報受発信サイト12は、利用者の属性別にアクセスの可否又はアクセス可能な情報を特定する属性別アクセス制御装置15と、利用者用コンピュータに向けて情報を発信すると共に利用者用コンピュータに入力されたデータを収集する情報受発信用サーバー16とを備えている。情報受発信用サーバー16は、例えば、データベースを駆動すると共にマークアップランゲージでのページを利用者用コンピュータに表示させるWebサーバーである。

【0020】属性別アクセス制御装置15は、演算装置であるCPUと、このCPUの主記憶となるRAMと、プログラムやデータを記憶するハードディスク等の補助記憶装置とを備えたコンピュータで実現できる。そして、属性別アクセス制御用のプログラムをそのCPUが実行することで、コンピュータは属性別アクセス制御装置として機能する。属性別アクセス制御用プログラムは、ネットワークを介して他のサーバーからダウンロードするようにしても良いし、図2の符号13で示すようなCD-ROM等の記憶媒体に格納し、プログラムをコンピュータまで搬送するようにしても良い。属性別ア

クセ制御用プログラムは、コンピュータで動作するオペレーティングシステムやサーバー用プログラム等に依存して、属性別アクセス制御装置として必要な機能及び手順を実現するための各種指令を備える。認証サーバ（他のコンピュータ）18についても同様に、認証サーバー用プログラムを記憶した記憶媒体14に格納された認証サーバー用プログラムを実行するコンピュータは、認証サーバー18として動作する。また、認証サーバー用プログラムを分割して他のサーバーからダウンロードして実行したり、認証サーバー自体を一つのノードとする分散環境下で認証サーバー用プログラムを実行させようにも良い。

【0021】図3は、図2に示した属性別アクセス制御システムの詳細構成を示すブロック図である。情報受発信サイト12は、利用者端末とのデータの送受信を制御するデータ送受信部32と、このデータ送受信部32を介して利用者端末と送受信するデータ又はプログラムデータからなる提供データの全部又は一部と当該提供データに対して利用者の年齢や在住地域等の属性別にアクセス可否を定めた属性別アクセス制御データとを記憶した属性別提供データ記憶部36と、利用者端末からデータ送受信部に提供データへのアクセスが要求された場合に属性別アクセス制御データに基づいて当該要求された提供データのアクセスに必要な属性の項目を当該利用者端末へ通知する属性項目通知制御部34と、認証サーバー22の認証要求属性データ出力部28によって出力される認証要求属性データに基づいて当該利用者のアクセスの可否を判定する属性項目別アクセス制御部30とを備えている。

【0022】データ送受信部32は、所定のプロトコルに従って利用者用コンピュータとページデータ等を送受信する。このとき、利用者用コンピュータ（利用者端末）毎のデータの送受信の可否については、アクセスの制御として属性項目別アクセス制御部30が制御する。また、送受信するデータは、ページデータ又はデータベースの形式で属性別提供データ記憶部36に格納されている。

【0023】この属性別提供データ記憶部36は、利用者端末と送受信するデータ又はプログラムデータからなる提供データの全部又は一部と、当該提供データに対して利用者の年齢や在住地域等の属性別にアクセス可否を定めた属性別アクセス制御データとを記憶している。利用者情報20と認証サーバー18との関係と同様に、提供データは、情報発信サイト内に設けても良いし、情報発信サイトと論理的に接続され、排他的にアクセス可能な位置に格納するようにしても良い。このため、提供データ記憶部36には、提供データの全部が格納される場合と、その一部としてのポインタのみが格納される場合などがある。

【0024】属性別提供データ記憶部36は、プログラ

ム又はデータからなる提供データのみならず、この提供データに対して利用者の年齢や在住地域等の属性別にアクセス可否を定めた属性別アクセス制御データを格納している。属性別アクセス制御データは、利用者からの全てのアクセスに対して一律の属性項目を指定するのであれば、例えば情報送受信サイトのホームページ（最初にアクセスされるページ又はデータ）については属性別のアクセス制御を行わず、他のページに対して一律の属性項目を指定するデータとなる。一方、個別の提供データ毎にアクセス制御をする場合には、例えば提供するページ毎にアクセス判定に必要な属性項目を属性別アクセス制御データとして記述する。

【0025】属性項目通知部34は、利用者端末10Aから要求されたアクセス種別に応じて、またはアクセスがあったときに一律に、アクセスの判定に必要な属性項目をネットワークを介して利用者端末10Aに通知する。例えば情報受発信サイト12がアクセスに年齢制限を有する場合には、通知する属性項目は年齢又は生年月日となる。また、情報受発信サイト12の特定のデータにアクセスする場合にのみ年齢制限がある場合には、属性別アクセス制御部30及び属性別提供データ記憶部36に格納された属性別アクセス制御データに基づいて利用者端末10Aへ通知する属性項目を特定する。

【0026】認証サーバー18は、利用者用端末から当該利用者の所定の属性についての証明要求を受信した場合に利用者情報から当該要求された属性に関する要求属性データを抽出する要求属性データ抽出部24と、この要求属性データ抽出部24によって抽出された要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証する要求属性データ認証部26と、この要求属性データ認証部26によって認証された認証要求属性データを外部出力する認証要求属性データ出力部28とを備えている。

【0027】認証サーバー18は、利用者情報20を管理する。この利用者情報は、例えばプロバイダやクレジットカード会社等への加入申込書等への記述と、利用者を個別に識別するために認証サーバーによって与えられた利用者IDとに基づいて作成すると良い。また、好ましい実施形態では、この利用者情報20は、本人によるアクセスのみを可能とするため、利用者から認証サーバー18へ向けたデジタル署名を用いると良い。要求属性データ抽出部24は、属性項目通知部34から通知された属性項目と、利用者端末10Aから送信された利用者IDとに基づいて、当該利用者IDと関連して格納された属性データを抽出する。このデータを、要求属性データと呼ぶ。続いて、要求属性データ認証部26は、デジタル署名等の手法を用いて、この要求属性データを認証サーバーにて認証する。例えば、要求属性データのハッシュを算出し、このハッシュ及び要求属性データを認証サーバーの秘密鍵で暗号化する。

【0028】認証要求属性データ出力部28は、このハッシュ等の認証用データを含み、必要に応じて暗号化されたデータを認証要求属性データとして外部出力する。利用者はこの認証要求属性データを情報受発信サイト12に転送する。情報受発信サイト12の属性項目別アクセス制御部30は、認証要求属性データを認証サーバーの公開鍵を用いて解読し、認証サーバーの認証が正しいことを確認する。すなわち、認証要求属性データが偽造されたものでなく、さらに認証後に変更されていないことを確認する。続いて、その属性項目の内容に基づいてアクセス可否を判定する。属性項目通知制御部34が、属性項目そのものでなく、属性項目でのある条件での問い合わせ文等として生成された場合には、認証サーバー22では、その条件を満たすか否かの論理型で認証要求属性データを生成するようにも良い。この場合、属性項目別アクセス制御部30は、認証要求属性データ中の論理型の記述に基づいてアクセス可否を判定する。

【0029】アクセス可否判定後、例えば、そのアクセスにより利用者端末10A及びデータ送受信部32にて生じたセッションを単位にアクセスを許可するようにしても良いし、また、アクセス管理用のIDを付与するようにしても良い。アクセス管理用IDを用いることで、利用者の匿名を保持したまま、一回又は複数回の接続を図1に示す属性別アクセス制御方法を用いて行うことができる。すなわち、利用者の属性を認証するためには利用者を特定しなければならないため、利用者端末10Aと認証サーバー22との間では利用者ID又はこれに対応するデータを用いなければならない。一方、情報受発信サイト12で要求しているのは、利用者の属性であって、利用者個人を識別する情報まで必要とはしない事態も想定しうる。また、匿名での世論調査などの場合には、利用者個人を識別可能な情報や、e-mailアドレスなどは情報受発信サイト12に送信しない方が望ましい。

【0030】一方、属性項目通知制御部34から属性項目の通知を受けた利用者と、その属性の証明を受けた利用者と、その後アクセスを継続する利用者との同一性を判定する必要がある。アクセス管理用IDは、この利用者の匿名を維持しつつ同一性を判定するためのもので、情報受発信サイト12によって生成され、認証要求属性データに含まれる。

【0031】このアクセス管理用IDを用いる例では、属性項目通知制御部30が、利用者のアクセスを制御するセッションや一定期間等の単位毎に他の利用者と識別するアクセス管理用IDを利用者端末へ向けて送信させるアクセス管理用ID送信機能40を備える。そして、認証サーバー22の要求属性データ認証部26が、認証要求属性データに情報受発信サイトによって発行されたアクセス管理用IDを含めるアクセス管理用ID付加機能42を備える。さらに、属性項目別アクセス制御部3

0は、認証要求属性データのアクセス管理用IDを使用する利用者に対してアクセスの単位分のアクセス権限を与えるアクセスID別管理機能38を備える。

【0032】アクセス管理用ID送信機能40は、利用者と情報受発信サイト12との通信を管理するためのアクセス管理用IDを発行し、利用者端末へ送信する。すると、認証サーバー22は、このアクセス管理用IDを含めた状態で認証要求属性データを生成する。この認証要求属性データにアクセス管理用IDを含めるため、利用者ID等の利用者の個人情報を含めずに認証要求属性データを生成することができる。そして、アクセスID別管理機能38は、アクセス管理用IDに対して、その属性項目の内容に応じたアクセス権限を付与する。これにより、利用者の匿名を保持しつつ利用者のネット上の自己申告よりは信頼性の高い属性情報に基づいてアクセスの制御を行うことができる。また、アクセス管理用IDを用いることで、予め定められた期間については一旦認証された属性項目でアクセス制御を行うことができる。

【0033】図3に示す例では、利用者端末10Aが直接ネットワーク1に接続される構成としたが、セキュリティを保持するための通信制御装置を介して接続したり、また、個人向けにインターネット等への接続サービスを行うプロバイダシステムを介して利用者端末10Aをネットワーク1に接続するようにしても良い。また、図3に示す認証サーバーの役割をプロバイダシステムが担うこととすると、個人情報の収集及び正確さの維持の点で現実的な利点がある。すなわち、個人がプロバイダに加入するには、加入申込書に個人情報を記載し、さらに決済を行うためにカード番号や銀行口座名等を記載する。また、プロバイダと加入者との間で郵便物の授受が行われるため、正確な現住所を得ることができる。これらの個人情報については、プロバイダは他の用途で利用することはできないが、上述した加入者の属性の保証を行うために、プロバイダでの加入者のIDを使用せずに属性保証のみを行うサービスに用いることについては、了承する利用者が多いと想定される。さらに、家庭で使用する場合、家族一人一人に属性証明用の利用者IDを付する場合には、成年者が未成年者の情報を記述する

（未成年者との契約には困難が多い）。このため、インターネットを利用する未成年者の年齢に関する属性情報が正確となる。従って、未成年者が見るべきでない提供情報を有するサイトが本実施形態による属性別アクセス制御機能を備えると、未成年の家族や同居者は有害な情報から未成年者を保護することができる。

【0034】図4は、プロバイダシステムが認証サーバーとして機能する場合の構成例を示すブロック図である。図4に示す例では、利用者端末10A、10B、10Cは、プロバイダシステム44を介してインターネットに接続する。インターネットには、属性別のアクセス

制御を行う情報送受信サイト12A、12Bとが接続されている。プロバイダシステム44は、利用者が利用できる有線又は無線の通信回線をインターネット網に接続するインターネット接続手段46と、利用者の氏名や年齢等の利用者個人情報を利用者識別用の利用者IDを単位として蓄積した利用者情報蓄積手段21と、利用者の個人情報の一部を利用者の属性として認証する認証手段48とを備えている。図3に示す認証サーバー22はその内部に利用者情報有する例を示したが、図4に示す例10では、認証サーバー22に対応する認証手段48に利用者情報蓄積手段21を併設する構成を示す。

【0035】認証手段48は、図3に示す認証サーバー22と同様に、利用者が利用する利用者用端末から当該利用者の所定の属性についての証明要求を受信した時に利用者情報から当該要求された属性に関する要求属性データを抽出する要求属性データ抽出部24と、この要求属性データ抽出部によって抽出された要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証する要求属性データ認証部26と、この要求属性データ認証部によって認証された認証要求属性データを外部出力する認証要求属性データ出力部28とを備えている。

【0036】インターネット接続手段46は、利用者端末10A、10B、10Cとの間で選択された通信回線を用いて利用者端末とプロバイダシステム44とを接続する。通信回線としては、アナログ又はデジタルの公衆電話回線や、携帯電話等による地上無線や衛星回線、また、CATV等の有線ケーブルなど、一般的にプロバイダシステムにて採用可能な種々の通信回線を含む。インターネット接続手段46はさらに、インターネット（インターネットと接続された他のコンピュータやルータ等）とプロバイダとを接続した専用線を利用者端末との通信に割り当てる。

【0037】認証手段48は、例えば利用者端末からプロバイダへダイヤルアップを行う際に利用者端末と接続されるようにしても良いし、また、1つの情報提供サイトの一機能として動作するようにしても良い。インターネット接続手段46と利用者端末10とは直接電話回線等を介して接続されるため、利用者用端末と認証手段48との間の通信のセキュリティを確保しやすい。図4に示す例では、プロバイダシステムに認証手段48を設けたが、属性項目別アクセス制御の処理工程は図1及び図3に示す例とほぼ同様である。

【0038】インターネット接続手段46により利用者端末10Aとインターネットを介した情報送受信サイト12Aとの接続が確立すると、情報送受信サイト12Aは、アクセス判定に必要な属性項目を利用者端末10Aに送信する。利用者端末10Aを使用している利用者は、利用者自身の属性の保証をプロバイダシステムの認証手段に要求する。具体的には、例えばプロバイダのホ

ームページから属性証明用ページにアクセスし、利用者用端末10Aに表示させる。利用者は、プロバイダに加入申し込みを行った際に例えれば家族一人一人に割り当てられた属性証明用のIDとパスワード等と共に属性項目の証明及び認証を要求する。続いて、プロバイダシステムの認証手段48は、属性証明用のIDとパスワードとから利用者情報蓄積手段21に格納された利用者の属性を読み出し、認証する。この認証を含むページを生成して利用者用端末に表示させたり、または、e-mailで利用者用端末へ送信する。利用者は、情報送受信サイトの所定の入力フィールドにこの認証手段48の認証要求属性データ出力部28によって出力された認証要求属性データを例えればコピーペーストする。情報送受信サイト12Aでは、この認証要求属性データに基づいて利用者のアクセスの可否を判定する。また、図3に示した各機能38、40、42を用いて、アクセス管理用IDを使用しても良い。

【0039】図3又は図4に示す認証サーバー22又は認証手段21は、属性認証用プログラムをサーバー用コンピュータにて実行することで実現できる。サーバー用コンピュータは、ネットワークに接続され、そして、利用者の属性別の個人情報を格納した利用者情報を管理する利用者情報管理部を備える。利用者情報管理部は、例えればデータベースとして格納された利用者情報の追加、更新、検索、削除等を管理する。そして、属性認証用プログラムは、サーバー用コンピュータを動作させる指令として、利用者用端末から送信された当該利用者の全属性のうちの一部の属性について証明を要求された場合に利用者情報管理部によって管理される利用者情報から当該要求された属性に関する要求属性データを抽出させる要求属性データ抽出指令と、この要求属性データ抽出指令に応じて抽出される要求属性データ又は当該要求属性データに基づいた判定結果を当該認証サーバーにて認証させる要求属性データ認証指令と、この要求属性データ認証指令に応じて認証される認証要求属性データを外部出力させる認証要求属性データ出力指令とを備えている。この各指令がサーバー用コンピュータにて実行されると、サーバー用コンピュータは、それぞれ要求属性データ抽出部24や、要求属性データ認証部26や、認証要求属性データ出力部28として動作する。

【0040】この属性認証用プログラムは、CD-ROM等の記憶媒体14に格納された状態で供給したり、又は、他のサーバーからネットワークを介してダウンロードすることができる。属性認証用プログラムは、サーバー用コンピュータのハードディスク等の補助記憶装置に格納され、サーバー用プログラム又はオペレーティングシステムのサービス上で実行される。このハードディスクも、属性認証用プログラムを格納した記憶媒体の一種である。この属性認証用プログラムが備えている各種指令は、コンピュータを動作させる指令であり、オペレ-

ティングシステム等のプログラム実行環境に依存した形態のコードで実現する。「動作させる指令」というときには、この指令のみで所定の処理を実現する場合と、サーバー用コンピュータに格納されたオペレーティングシステムやサーバー用プログラムによるサービスに依存して所定の処理を実現する場合との双方を含む。例えば、「要求属性データ抽出指令」は、Webサーバーが有しているデータベース管理サービスに利用者IDとデータベース上の項目名とを引き渡す指令のみであってもよい。

【0041】また、サーバー用コンピュータで実現すべき機能に応じて、属性認証用プログラムは、その機能に応じた指令を備えると良い。例えば、情報送受信サイト12Aがアクセス管理用IDを用いて属性項目の証明を要求する場合には、要求属性データ認証指令は、利用者用端末から属性の証明をされる際にアクセス管理用IDが付されていた場合には当該アクセス管理用IDを認証要求属性データに当該アクセス管理用IDを含有させる指令を備えると良い。これにより、サーバー用コンピュータは、アクセス管理用ID付加機能を実現する。

【0042】上述したように本実施形態によると、プロバイダシステム又は認証サーバーが予め定められた利用者情報に基づいて、要求された属性項目の内容を保証するため、情報受発信サイトにて利用者の属性別に正確なアクセス制御を行うことができる。また、利用者側でも、利用者自身の個人情報を情報受発信サイトに知らせずに、年齢別や性別等の属性に応じた情報の授受が可能となる。さらに、例えは成人向けの情報を含む情報受発信サイトがこの属性別アクセス制御方法を採用することで、インターネットを利用する子供達を悪影響から保護することができる。また、在住地域別の世論調査や、特定地域在住で且つ選挙権を有する年齢であることを証明しつつ、無記名で（すなわち、匿名で）ネット上で選挙を行うための基礎技術の一つとなる。

【0043】

【実施例】次に、図5乃至図8を参照して、本発明の実施例を説明する。図5は本実施例の概略構成を示すブロック図である。図2及び図3に示す構成の内、主要な部分を簡略化して示している。情報受発信サイト12には、属性別提供データ記憶部36が併設されている。一方、認証サーバー22（またはプロバイダシステム44の一部）には、利用者情報20が併設されている。利用者用コンピュータ（または利用者端末）を、ここでは利用者クライアントと呼ぶ。

【0044】情報受発信サイト12は、不特定多数の利用者に対して情報提供等のサービスを行う。情報受発信サイト12は、利用者に対して個人情報の公開を要求はないが、ある属性について一定の条件を満たすことだけを要求する。さらに、情報受発信サイト12は、利用者クライアント10に対して証明を要求する属性が何で

あるか等の情報を含む属性証明要求50を送信する。【0045】利用者は利用者クライアント10を操作して、利用者が加入している保証者の認証サーバー22へ、属性保証要求51を送信する。保証者は、何種類かの属性に関して利用者の情報を予め所持している。また、一般的には、利用者からの依頼でなければ情報を開示しない旨を利用者に約束することが望ましい。認証サーバー22は、属性保証要求51が確かに利用者からのものであることを確かめた上で、利用者のデータを参照し要求された属性に於ける利用者の属性値の入った認証要求属性データ52を利用者クライアント10へ送信する。

【0046】利用者は、利用者クライアント10を操作して、情報受発信サイト12に対して開示しても良い属性の属性値しか含まれていないことを確認した上で、認証要求属性データ52の内容が入った属性証明データ53を作成し、情報受発信サイト12へ転送する。

【0047】情報受発信サイト12は、属性証明データ53の内容に基づいて、自らが発行した属性証明要求50に対応するものであることと、信頼できる保証者が発行した保証であることとを確認した上で認証を完了し、アクセス制御を行う。

【0048】次に、動作例を説明する。図6及び図7は本実施例で使用する各種データ等の例を示す説明図である。属性証明要求50の内容50aは、図6(A)に示す例では、要求の対象である属性の名前(図6に示す例では生年)の他に、その時1回限りの文字列を含んでいる。この1回限りの文字列は、上述した実施形態でのアクセス制御用1Dに対応する。この1回限りの文字列を用いると、利用者の匿名性保護に更に役立つ。

【0049】図8は情報送受信サイトが属性項目を利用者に送信した例を示す説明図である。図8に示す例では、世論調査を行うための情報送受信サイトが、属性項目及び1回限りの文字列をHTMLページ12Aとして生成し、利用者クライアント10に送信している。図8に示す例では、要求者発行番号としているが、これは本実施例の一回限りの文字列であり、上述した実施形態ではアクセス管理用1Dである。この世論調査の例では、生年月日と現住所とをアクセス可否の属性項目としている。

【0050】利用者クライアント10は、情報受発信サイト12からの要求の表示と、保証者の選択、保証依頼の送信をサポートする。利用者は自らが加入している保証者を選択するかまたはそのアドレスを入力するなどにより、属性保証要求51を保証者に送信する。属性保証要求51の内容51aには、図6(B)に示すように、利用者が保証者に対して所有する利用者1Dと、保証して欲しい属性の名前(図6に示す例では生年)と、前述の1回限りの文字列の他に、利用者の署名を付ける。この利用者の署名を付することで、認証サーバー22は利用

者本人であることを認証することができる。

【0051】図9は認証サーバー22での属性保証を行うための利用者向けユーザインタフェースを示す説明図である。図9に示す例では、プロバイダシステムは属性保証ページを生成し、利用者クライアントに表示させ、属性保証要求51をe-mailにて受信することとしている。また、利用者情報の項目に応じて属性保証を行える項目が限定されることから、その一覧を表示し、利用者の選択を促すこととしている。また、要求者発行番号については、ページ内に入力フィールドを設けている。図9に示す例では、利用者を加入者と称呼しているが、これはプロバイダにとって利用者はプロバイダの提供するサービスに加入した者であるためである。上述した家族で1つのプロバイダを使用することもあるため、送信時のe-mailにて加入者の署名を得ることとしている。この図8及び図9に示すユーザインタフェースは、現状のWebサーバーとHTMLによるページの表示という技術に応じて本実施例の理解を容易とするための例であり、本発明はユーザインタフェースの具体例によって限定されるべきものではない。

【0052】認証サーバー22は、図7(C)に示すように、利用者1人ずつに対して公開鍵、各種属性値の入ったデータベースを所有している。属性保証要求51(例えばe-mail)に付加された利用者の署名を利用者の公開鍵で復号化し、属性保証要求51が確かに利用者からの依頼であることを確認する。また、認証サーバー22は、利用者クライアント10に対して認証要求属性データ52を送信する。この時、認証要求属性データ52の内容52aには、図6(C)に示すように、保証者の署名を付加し、利用者の属性値(図6に示す例では1978年)を含めると良い。また、好ましくは、前述の1回限りの文字列を含み、利用者1Dを含まない様にすると良い。

【0053】情報受発信サイト12側は、自らが発行した要求に対応する保証であることさえ確認できれば充分であり、当該利用者が当該保証者に対して所有する利用者1Dなどは要求していない。これにより、情報受発信サイト12が利用者を同定できないことが利用者にも確認できるので、利用者の匿名性保護に更に役立つ。

【0054】利用者クライアント10は、認証要求属性データ52の内容の確認をサポートすると良い。すなわち、本実施例では、図7(B)に示すように、利用者は、認証要求属性データ52の中に開示を望まない情報が入っていないことを目視で確認する。利用者クライアント10は利用者の操作に応じて認証要求属性データ52と同内容の属性証明データ53を情報受発信サイト12へ転送する。

【0055】情報受発信サイト12は、図7(A)に示すように、信頼できると判断する幾つかの保証者の名前と公開鍵の組合せを所持している。情報受発信サイト1

2は属性証明データ53の内容を読み、保証者の署名を保証者の公開鍵で復号化し、保証の内容が確かに保証者のものであることを確認する。保証された属性値が情報受発信サイト12の要求した条件を満たしていれば認証は完了する。

【0056】図6(C)を参照して、本実施例での認証要求属性データについて再度説明する。認証要求属性データは、認証サーバー22によって認証されており、その属性データは、情報受発信サイト12にてアクセス管理用IDを用いた利用者のアクセス制限の判定に用いられる。従って、認証要求属性データは、情報受発信サイトにて属性別のアクセスを制御するための属性別アクセス制御データとして機能する。この属性別アクセス制御データは、情報受発信サイト12に利用者用端末10を用いてアクセスした利用者に割り当てられるアクセス管理用IDデータ(本実施例では、1回限りの文字列)52dと、情報受発信サイト12によって特定された利用者用端末を使用する利用者の属性項目データ(属性名を示すデータ)52bと、この属性項目データ52bにて指定される項目について認証サーバーの利用者情報から抽出された属性データ(属性値)52cと、各データの内少なくとも属性データ52cの内容を認証サーバーにて認証したことを証明するための認証用データ(例えば、保証者の署名)52eとを備えている。

【0057】アクセス管理用IDデータ52dは、図6(C)に示す例では、「a b c 1 2 3」であり、属性項目データ52bは、「生年」であり、その属性値52cは1978年である。認証要求属性データが、一回限りの文字列52dと、属性値52cとを備えたため、利用者を識別するための利用者ID等を含まずに、属性別のアクセス制御が可能となる。従って、利用者はこの認証要求属性データを用いることで、利用者本人の署名を保持しながら属性別にアクセスを制御する情報受発信サイト12に属性値を通知することができる。情報受発信サイト12は、この属性値に基づいて属性項目に対する条件を満たしているか否かを判定し、この判定結果に基づいてアクセスの可否を制御する。

【0058】また、図6(C)に示す形式ではなく、情報受発信サイト12から、属性項目の属性値に対する条件が発行される場合には、属性値ではなく当該属性項目の条件を満たしているか否かのデータを認証要求属性データに含めるようにしても良い。この場合、属性項目に対する条件を満たしているか否かの判定を、認証サーバー22にて行うこととなる。この例では、情報受発信サイトに利用者用端末を用いてアクセスした利用者に割り当てられるアクセス管理用IDデータと、情報受発信サイトによって特定された利用者用端末を使用する利用者の属性項目データと、この各属性項目データに対して情報受発信サイトによってそれぞれ与えられる条件データと、この各属性項目データに対して与えられた条件データ

タによる条件を満たしているか否かを認証サーバーの利用者情報に基づいて判定した属性項目別判定結果データと、各データの内少なくとも属性項目別判定結果データの内容を認証サーバーにて認証したことを証明するための認証用データとを備える。

【0059】属性データ及び属性項目データは、例えば、データベースに対する問い合わせ文として記述することができる。例えば年齢であれば整数の大小関係として記述することができ、また、住所等であればある文字を含むか否かの問い合わせ文として記述することができる。属性項目別判定結果データは、例えば真又は偽の論理型の値で記述することができる。

【0060】次に、図10を参照して、Java(商標)関連技術を用いた実施例を説明する。サイト用Webサーバー60は、図5に示す情報受発信サイト12として動作する。提供データデータベース(提供データDB)は、属性別提供データ記憶部36として機能する。認証用Webサーバー62は認証サーバー22に対応する。利用者情報DB64は、図5に示す利用者情報20をデータベースとして設けたものである。Javaアプレット63は、このJavaアプレット63をダウンロードし、JavaVM(ヴァーチャルマシン)として機能するコンピュータを駆動する。一般的な利用者用コンピュータ10であれば、インターネットを介したページの受信や、Javaアプレット63の実行をWebブラウザにて行う。また、図10では、Javaの実行環境を有する組込機器(利用者用機器)65を用いて行う場合を、JavaVM66として示した。

【0061】認証用Webサーバーにて管理されるJavaアプレット63は、利用者用機器65や利用者用コンピュータ10にてダウンロードされ、実行される。この例では、利用者用コンピュータ10や利用者用機器65にはなんら特別なプログラムを設げずに、Javaの実行環境を備えるのみで属性別アクセス制御方法を実施することができる。Javaアプレット63は、例えば、図7(B)に示す利用者クライアントでの各種操作を実現させる。

【0062】利用者は、サイト用Webサーバー60にアクセスすると、例えば図8に示すページ等により属性項目が通知される。統いて、利用者は、認証用Webサーバー62にアクセスし、図9に示すページやJavaアプレット等をダウンロードする。そして、認証用Webサーバー62に属性保証要求51を送信する。認証用Webサーバーは、属性保証要求51に応じて利用者情報DB64から属性値を抽出し、認証要求属性データ52を生成する。そして、利用者用コンピュータ10にダウンロードされたJavaアプレットは、要求された属性以外の情報が入っていないことを利用者に表示した上で、当該認証要求属性データ52をサイト用Webサーバーに送信する。サイト用Webサーバーでは、認証要

21

求属性データ52を用いて、提供データDB61等からページを生成又は読み出して利用者用コンピュータ10に送信する。利用者用コンピュータのWebブラウザ67は、サイト用Webサーバー60から送信されたページを表示する。

【0063】

【発明の効果】本発明は以上のように構成され機能するので、これによると、属性保証データ生成工程にて、利用者情報に基づいて利用者の属性項目の内容を保証する属性保証データを生成し、属性証明データ送信工程にて、属性保証データを利用者用コンピュータは利用者の属性を証明する属性証明データとして属性別アクセス制御装置に送信するため、すなわち、他のコンピュータにて保証された属性保証データを用いて属性別アクセス制御装置に対して利用者の属性の内容を証明することができ、すると、属性別アクセス制御装置は、他のコンピュータにて保証された属性内容に基づいて利用者のアクセスを制御することができ、このため、利用者の自己申告に依存せずに正確な利用者の属性をアクセス管理のために得ることができ、すると、不特定多数を対象とする情報受発信サイトにて利用者の年齢や性別などに応じた情報の受発信を行うことができる、という従来にない優れた属性別アクセス制御方法及びシステムを提供することができる。

【図面の簡単な説明】

【図1】本発明の一実施形態の構成を示すフローチャートである。

【図2】図1に示す属性別アクセス制御方法の実施に好適な属性別アクセス制御システムの構成例を示すブロック図である。

【図3】本発明による属性別アクセス制御装置の一実施形態の構成を示すブロック図である。

【図4】本発明によるプロバイダシステムの一実施形態の構成を示すブロック図である。

【図5】本発明の一実施例の概略構成を示すブロック図である。

【図6】図5に示した構成にて使用する各種データの例を示す説明図であり、図6(A)は属性証明要求の内容

22

例を示す図で、図6(B)は属性保証要求の内容例を示す図で、図6(C)は認証要求属性データの内容例を示す図である。

【図7】図5に示した各構成にて使用するデータ等の例を示す説明図であり、図7(A)は情報受発信サイトが使用するデータベースの一例を示す図で、図7(B)は利用者クライアント上でサポートする操作の例を示す図で、図7(C)は認証サーバーが保持するデータベースの一例を示す図である。

【図8】本実施例での情報受発信サイトが利用者へ属性及びその条件を通知するためのユーザインターフェースの一例を示す説明図である。

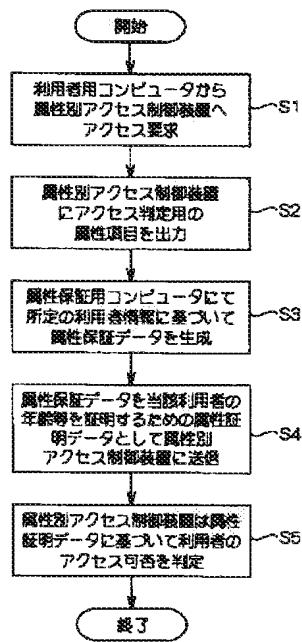
【図9】本実施例での認証サーバー(プロバイダシステム)が利用者へ属性証明要求のための入力を促すためのユーザインターフェースの一例を示す説明図である。

【図10】Java関連技術を用いた実施例の構成を示すブロック図である。

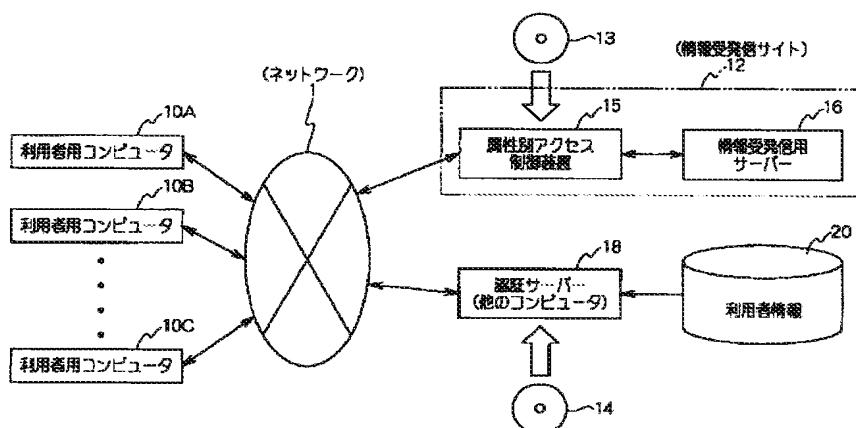
【符号の説明】

- 1 ネットワーク(例えば、インターネット)
- 20 10, 10A, 10B, 10C 利用者用コンピュータ(又は利用者端末や組込機器)
- 12 情報受発信サイト
- 15 属性別アクセス制御装置
- 16 情報受発信用サーバー
- 18 他のコンピュータ(例えば、認証サーバーやプロバイダシステム)
- 20 利用者情報(又は、利用者情報記憶部)
- 22 利用者情報を含む認証サーバー
- 24 要求属性データ抽出部
- 30 26 要求属性データ認証部
- 28 認証要求属性データ出力部
- 30 属性項目別アクセス制御部
- 32 データ送受信部
- 34 属性項目通知制御部
- 36 属性別提供データ記憶部
- 38 アクセスID別管理機能
- 40 アクセス管理用ID送信機能
- 42 アクセス管理用ID付加機能

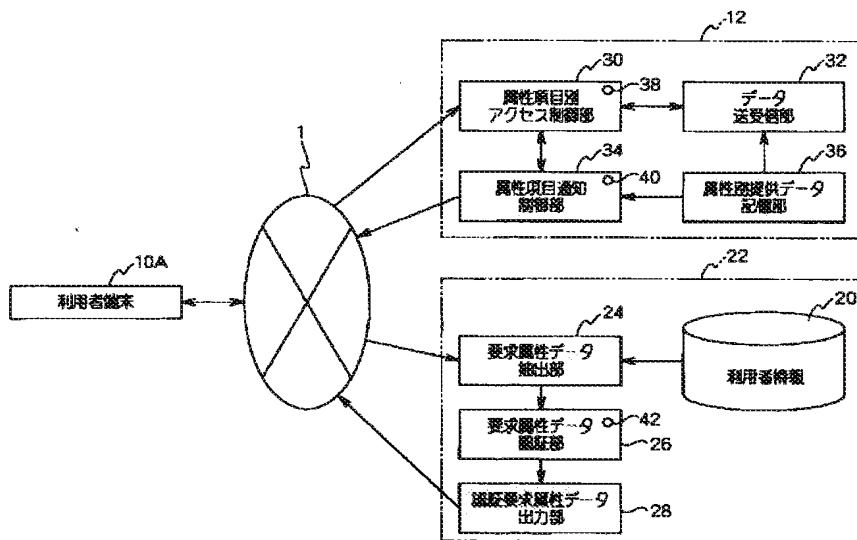
【図1】



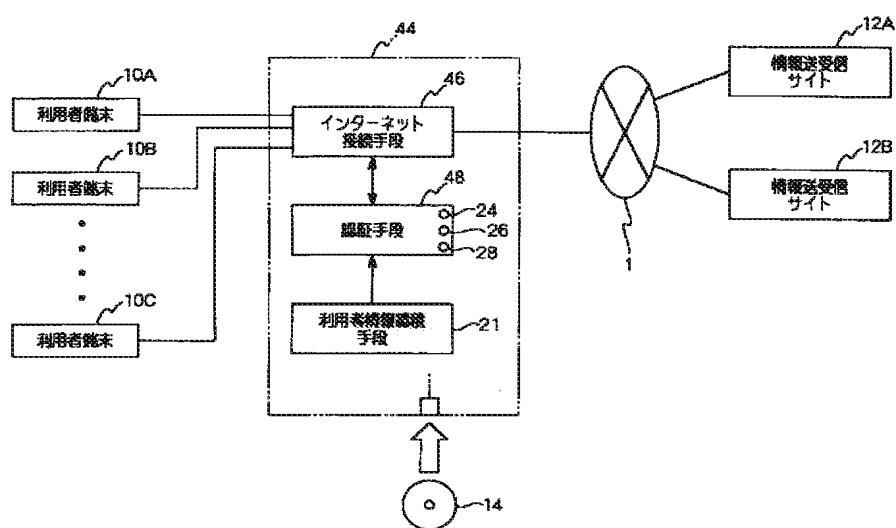
【図2】



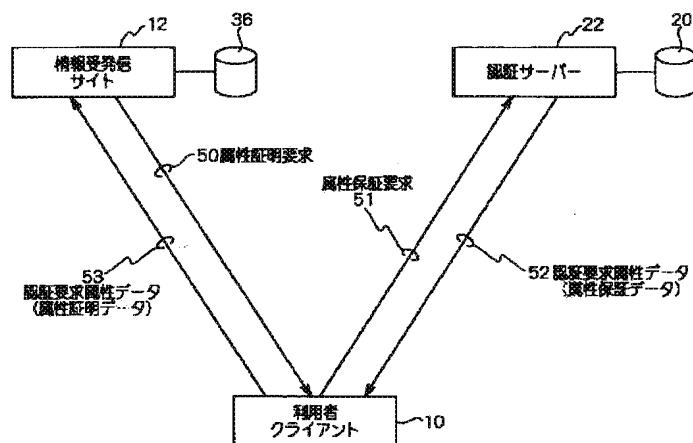
【図3】



【図4】



【図5】



【図6】

属性証明要求の内容：
 属性 : 生年
 1回限りの文字列 : abc123

(A)

属性保証要求の内容：
 利用者id : user1
 属性 : 生年
 1回限りの文字列 : abc123
 利用者署名 : ~~

(B)

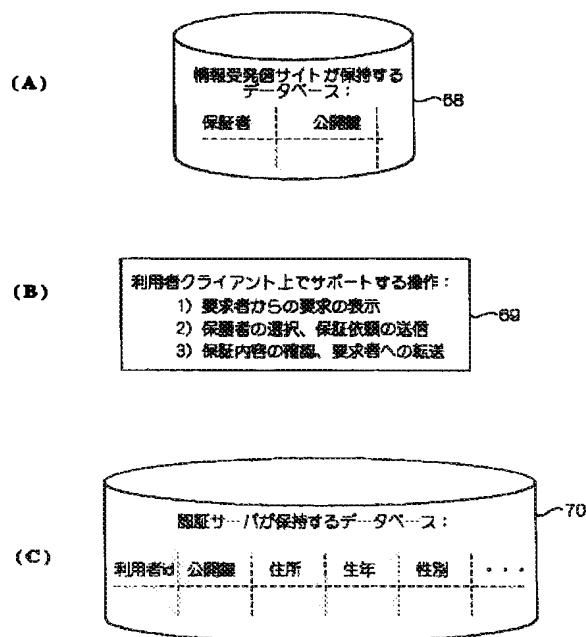
認証要求属性データの内容：
 属性 : 生年
 属性値 : 1978年
 1回限りの文字列 : abc123
 保証者の署名 : ~~

(C)

【図8】

【図8】のウェブページのスクリーンショットを示す。画面には「こちらは〇〇市の世論調査のページです。本調査は匿名でご応募いただくのですが、貴方の属性について」のメッセージが表示されている。下部には「生年月日」が「1980年3月24日以前」と入力された状況、「居住地」が「〇〇市内」と入力された状況が示されている。また、「の証明を送付して下さい。要求者発行番号は chhd-508142 です」と記載されている。

【図7】



【図9】

18A

こちらはXXプロバイダの属性保護のページです。
加入者の皆様が、何処かのサイトで属性証明を要求された場合は
以下の欄に記入して属性保護を取って下さい。

加入者番号 : GTT666310

保護を要する属性: 以下から選択して下さい。

<input checked="" type="checkbox"/> 生年月日	<input type="checkbox"/> 性別
<input type="checkbox"/> 国籍	<input checked="" type="checkbox"/> 現住所
<input type="checkbox"/> 学生・社会人の別	<input type="checkbox"/> 会社名
<input type="checkbox"/> 扶養家族の有無	<input type="checkbox"/> ~~

属性証明を要求したサイトが表示した、要求者発行番号を記入して下さい。
chid-508142

上記の内容に記入なさった後、下の送信ボタンを押して下さい。
送信

上のボタンを押下すると、XXプロバイダへのメールの送信画面になります。
貴方が上記の加入者本人であることを証明する署名をつけて送信して下さい。

【図10】

